

REAL TIME ACTIVE NETWORK COMPARTMENTALIZATION

DESCRIPTION

BACKGROUND OF THE INVENTION

Cross-Reference to Related Applications

5 This application claims priority of U. S.
Provisional Application S. N. 60/248,906, filed
November 15, 2000, and assigned to the assignee of
the present application, as does concurrently
filed related application 09/____,____, (Docket
10 Number FS-00510 (02890038AA)) both of which are
hereby fully incorporated by reference.

Field of the Invention

15 The present invention generally relates to
digital communications networks and, more
particularly, to the development of the properties
of high levels of security and fault tolerance by
active attack detection and real time
establishment of compartmented security domains to
permit network functionality in the presence of
20 denial of service and other attacks.

Description of the Prior Art

Numerous technical developments and economic
forces have led to the widespread use of
distributed data processing systems in which
25 numerous data processors, each of which may be
capable of functioning independently, are
connected by a network in order to share both data
and hardware and software resources. The
connectivity of the system may be hard wired over

T0T0T0T-#224E2663

a local or wide area network or may use links which are more or less accessible to the public, such as the Internet which utilizes many common carrier communication links which may be made available to a given processor through various hardware interfaces. When such technical capabilities such as the development of the TCP/IP protocol were being initially developed, however, flexibility of interconnectivity, scalability and ease and reliability of data exchange were of paramount importance and the importance of security measures was not fully appreciated and left to be implemented at individual processors or individual resources to prevent access from other connected processors.

Of course, a given processor may be effectively connected to more than one network at a time and thus a publicly accessible network can be used to access another network, potentially through a sequence of processors. On the other hand, limiting access of processors to only secure or unsecure networks reduces functionality of the processor to levels which may be unacceptable due to the reduction of accessible resources. It is also in the versatile nature of data processors that any security feature that may be devised may also be defeated and protection of sensitive resources is entirely grounded in the difficulty of defeating the security measures utilized.

Further, as alluded to above, restriction of access is usually provided only at individual processors or resources (e.g. applications) and not within the network, itself.

As the use of TCP/IP networking has grown, techniques for exploiting a lack of security have been discovered, developed, implemented and widely shared in the hacker community worldwide. This

TOP SECRET//SI//FOUO

circumstance presents a fundamental threat to the global network infrastructure that must be ameliorated if security of any network or connected resource is to be achieved.

5 Accordingly, there are numerous reports of increasingly sophisticated intruder attacks on both military and commercial computer systems. Computer attacks may take the form of gaining access to sensitive data (to either learn its 10 contents or to corrupt it) resident on individual systems or in the form of a so-called virus or worm to damage or destroy processors or resources in a largely indiscriminate manner.

15 Yet another form of attack which is of increasing concern is the "denial of service" (DOS) attack in which normal network functions are demanded at rates approaching or exceeding system capacity to respond, thereby denying service to other requestors or otherwise disrupting other 20 communications or services such as overloading telephone or power distribution networks. It has also been reported by numerous studies that many such attacks, regardless of form, are initiated by persons having some level of legitimate authorized 25 access to the system attacked or at least a connected system.

30 Networks are inherently susceptible to attack by exploitation of security weaknesses in network protocols and infrastructure components. In addition to unauthorized viewing and modification of data, alluded to above, security controls of the operating systems and applications installed on the network may be circumvented, network firewalls (used extensively at network boundaries) 35 may be penetrated, network functions may be disrupted, sessions of authorized users (after they have been authenticated) can be stolen and

TOP SECRET//SI//E//FOB

routing functions of the network can be disrupted to misdirect network data. A concerted attack on military network infrastructure can compromise military operations or force network shutdown.

5 Identification and authentication (I&A) capabilities provided by recently developed forms of identification certificates does not provide technical mechanisms to respond to attacks against network protocols.

10 Traditionally, a three layered approach has been taken in an attempt to provide protection of networks. The first layer is the extensive use of firewalls to control access to the network from outside the network. However, firewalls become 15 geometrically more difficult to manage as the number and variety of authorized accesses increases. This difficulty is particularly evident in military networks which become particularly susceptible to penetration through 20 exploitation of errors in configuration of their access control rule set.

However, firewalls are not fully effective since the manner in which TCP/IP manages packet fragmentation can be exploited for "punching 25 through" the packet filtering system of firewalls. "Session Hijacking", although complex, can be automated to negate effective use of strong user authentication. Further, it is difficult to force all network access to be made only through the 30 firewall. The availability of commercial modems that interface to digital PBX systems and the Remote Access Server included in Microsoft Windows (TM) software makes control of the use of dial-up connections to the network through firewalls 35 impractical.

The second layer of protection is strong user authentication such as biometric systems and

TOP SECRET//EYES ONLY

digital certificates. However, such systems are costly and generally implemented on only the most sensitive systems and can, nevertheless, be rendered ineffective by session hijacking attacks,
5 alluded to above, because of the inability of TCP/IP to authenticate the source address packets, to close out "half-open" connections and to protect the session sequence numbers contained in the TCP header.

10 The third layer of protection is to maintain separate networks for each level of security classification or class of access authorization and to depend on personnel clearances. This approach is extremely costly, limits the
15 functionality of each separate system, presents problems of maintaining data integrity and provides no protection from misuse or damage by persons having access to any given system.
Further, it is generally desirable to be able to accommodate both mandatory access control (MAC) in which access is controlled based on classification of the information or resource and discretionary access control (DAC) which is based on a correlation of anticipated user function and the
20 nature of data that may be needed to perform that function. It can be readily appreciated that MAC and DAC may each be complex and overlap with much increased complexity, greatly multiplying the
25 number of separate systems which may be required among which data integrity must be maintained.
30

35 Detection of an attack before substantial damage is done is often difficult, particularly when the attack is of the denial of service type. Viruses, for example, cannot be detected before at least some of their basic characteristics (e.g. a filename by which they are executed) is known; by which time the virus may have been widely

TOP SECRET//EYES ONLY

proliferated, causing some degree of damage to each computer it has reached. A denial of service attack is, by its nature, indistinguishable from other intended functions of the system except for
5 the volume of transactions it presents and possible similarities of requested services necessitated by the volume of requests required for a successful attack.

In general, when an attack is detected, at least a major portion of network services must be disrupted in order to respond to the attack. Therefore, achieving a degree of certainty that an
10 attack is in progress commensurate with the magnitude of necessary system disruption often
15 unacceptably delays action and thus does not acceptably limit damage or prevent access to critical data or resources.

In summary, enhancement of security in digital networks is extremely challenging in view of the weaknesses in protocols which cannot readily be changed. Most approaches proposed to date are extremely costly and compromise system functionality and utility while being difficult to implement in complex environments that cannot
20 readily be modified. Proposals for security enhancements to date have also not been easily scalable, potentially functional across multiple networks or globally, adequately sensitive to potential attacks, capable of accurately and
25 quickly isolating a fault or an attack and allowing error recovery or able to actively protect against attacks by authorized users, the currently most frequent source of system attacks.
30

TOP SECRET//EYES ONLY

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide fault and potential attack encapsulation in a fine-grained manner in a digital communications network.

5 It is another object of the invention to provide error and damage limitation and recovery in a rapid and automatic manner in a digital communications network to rapidly restore the full 10 functionality thereof quickly and with minimal disruption.

15 It is a further object of the invention to provide a global active response to faults and potential attacks in substantially real time while maintaining substantially undiminished network capabilities.

20 In order to accomplish these and other objects of the invention, a method of operating a digital network having nodes which have a locally hierarchical relationship is provided comprising steps of detecting a condition at a node and communicating the condition to a trusted node locally higher in the hierarchical relationship, collecting information regarding the condition 25 through nodes at the same or higher hierarchical level as said trusted node, and controlling a response at the node in response to the information.

T00707-9722660

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, in which:

Figure 1 is a schematic diagram of a basic element of the network in accordance with the invention and including a lock circuit including two routers providing communications from different networks,

Figure 2 is a schematic illustration of a redundant hierarchy of independently secured security domains in accordance with the invention,

Figure 3 schematically illustrates an exemplary preferred operation of the redundant hierarchy of Figure 2, and

Figure 4 illustrates an exemplary global search technique for potentially compromised nodes of a network.

DETAILED DESCRIPTION OF A PREFERRED
EMBODIMENT OF THE INVENTION

Referring now to the drawings, and more particularly to Figure 1, there is shown a basic network element 103 and associated network nodes in accordance with the invention. It should be understood that routers are well-understood network elements for controlling communications between nodes of a network although only a single router (but which may have an arbitrary number of ports) would normally be associated with a given node of the network. Use of a lock in combination with routers is also well-understood in the art. However, it should be understood that no portion of any Figure is admitted to be prior art in regard to the present invention.

As will become clear from the following discussion, the present invention provides a secure, fault-tolerant network than can implement an arbitrary security policy with arbitrarily fine granularity and continue to provide service in the presence of a variety of hardware failures and security penetration attacks. This is accomplished by developing a networking subsystem by inclusion of enhancements which accommodate existing elements of network architecture and software and integrate fault tolerant extensions of object oriented programming architecture, strong encryption strong authentication at the node and data packet level and real-time active responses to detection of faults and attacks with enhanced sensitivity.

It should also be appreciated that while the preferred form of the invention will be discussed in the context of well-known standard protocols and a preferred common object request broker

00000000000000000000000000000000

architecture (CORBA, an architecture that, including extensions such have been made commercially available by the assignee of the present invention under the name "Hardpack" for developing a high degree of fault tolerance, such as repairing or replacing software objects from other nodes when needed, as is summarized in the above-incorporated U. S. provisional patent application, enables modules of software, known as "objects" to communicate with one another) and common management information protocol (CMIP, an open system interconnection (OSI) standard protocol used with common management information services (CMIS) standard protocol) other architectures and protocols may be used to embody the invention.

As will be discussed below, the basic principle of the invention is the use of a highly secure user transparent subsystem infrastructure which can detect failures and questionable activity and communicate, in a secure and encrypted form, the potential condition of a network node to adjacent nodes which can then isolate or encapsulate a potentially compromised node while rerouting normal network traffic to integrate the extended and fault tolerant CORBA architecture with strong encryption, enhanced intrusion detection and an effective security policy to support effective active responses to faults and potential attacks. This reporting supports fine-grained control of network access as well as logging of information concerning network activity and node status to limit damage, improve detection and facilitate recovery from a wide variety of failures and attacks.

As shown in Figure 1, the overall function of the interface element 103 including two locking

devices 109, 111 and two routers 105, 107 is to support communications with and between networks 115, 117 through routers 105, 107 and with network node 119 which may or may not also include a similar interface element. Thus, it can be appreciated that interface element 103 can control the connectivity of three network nodes. Further, it can be appreciated that locking devices 109, 111 communicate with each other to provide connectivity between networks 115, 117 as well as with processor 119. Thus, the interface element 103 can function as a lock to interrupt communications between networks, nodes or terminals at a particular network node.

Locking devices are generally implemented on separate cards (a preferred form of which is known as a VME card) which are connectable to other circuits through a rack or "motherboard" arrangement or the like. Therefore, it is convenient to provide additional security structure at a location electrically between the two locking devices (e.g. connected to a common bus). In accordance with the invention, this is preferably accomplished with a processor on a separate card (represented by 113 of Figure 1) processing fault and intrusion detection objects as well as encryption and decryption algorithms for communication of data regarding potential faults and attacks to similar cards at other network nodes. Thus it is seen that the basic element of the invention can be mechanically assembled and integrated into a system in a simple and convenient manner while not affecting other parts of the network or normal functions thereof. Accordingly, implementation of the invention can be performed incrementally and scalably to any desired degree including global implementation.

Functionally, it should be appreciated that the processor arrangement 113 can implement any number of objects for fault or intrusion detection and which may be of any arbitrary design, including a number of algorithms which are commercially available for the purpose. Results of the execution of these objects can be communicated over normal network links to other nodes and used by manager objects to exercise any desired control over the locking devices, to implement any desired security policy (e.g. mandatory access control (MAC), Discretionary access control (DAC), and the like) and/or to log any desired information concerning the status or operations of any node through other managed objects at each node. More generally, managed objects include network interface managed objects, intrusion detection managed objects and network service managed objects.

All of these communications are preferably performed in a user transparent fashion at high bit rates and encrypted in accordance with any desired encryption algorithm (DES, DES-3 or Type 1 algorithms implemented in hardware for highest speed being preferred) which may also be altered and keys arbitrarily exchanged and altered by the same type of communications which are entirely transparent to all users and may be made arbitrarily difficult to intercept by any of a number of known techniques which will be evident to those skilled in the art. Further, each transmission or group of transmissions for a given user) may be supplied with identification information (e.g. in the form of a stamp or the like) by processor 113, even if the user is not identified and any desired tracking or logging information may be transmitted to other nodes for

error recovery and determination of the source of any detected potential attack as well as continuous monitoring and authentication of the source node for all communications, potentially to the data packet level.

These detection operations and communications may be conducted separately from normal user data communications traffic in substantially real time and communications performed at extremely high

data rates potentially as great as or exceeding 10 Gbps since it is essentially only necessary for boards 113 at different network nodes to be compatible and communicate with each other and with complete independence from other user data

communication processors connected to the network. High transmission bit rates and, preferably, transmission priority arrangements for such user transparent network infrastructure communications (e.g. preferentially communicated relative to user data communications) assist in assuring that network security control functions will be carried out even during denial of service (DOS) attacks. Accordingly, the processor card 113 is referred to as a security policy manager (SPM) card.

It should be appreciated that implementation of such capabilities in combination with routers which also support a high level of security (e.g. cards supporting audit, MAC, DAC, user identification and authentication security functions) enables active network response to security alerts and isolation of compromised nodes from uncompromised nodes in substantially real time (often referred to as log time since the actual time required is a fixed multiple of the logarithm of the number of the nodes secured and thus increases slowly as the number of nodes increases and the granularity of protection is

TOP SECRET//COMINT

made finer) as will be discussed in more detail below. Further details of the preferred implementation of this basic element of the invention are disclosed in greater detail in the above-incorporated, concurrently filed U. S. Patent Application.

Referring now to Figure 2, a network 401 is shown hierarchically arranged in tiers 403, 405, 407 with communications paths (e.g. 415, 423) shown connecting respective adjacent tiers. While a hierarchy of tiers is preferred and illustration of communication links limited to those between respective adjacent tiers as a matter of clarity, it is only necessary to the successful practice of the invention that any given tier have more than one node or a communication path past that tier and a tier at a locally higher hierarchical level. Even these requirements are only necessary to the extent of providing an orderly correspondence between manager objects and managed objects; which correspondence could be accommodated in other ways that provide a locally hierarchically higher node for each node except for the highest tier. Other network configurations are also possible and may be desirable under particular circumstances or for particular applications.

For example, a communication link depicted by dashed line 430 could be used as a communication link through tier 405 with tier 407 above tier 403 or to place a node of tier 403 hierarchically above tier 407. Nevertheless, an organization containing communications links such as 430 may engender unjustified complexity although some advantages may accrue such as establishing further redundant communication paths and/or avoiding a top level of the hierarchy which might be an excessively attractive target for attack.

TOP SECRET - 12/27/96

It should be noted that the network shown in Figure 4 (without link 430) provides redundant communication links between all nodes of the network even though there are no links between nodes of the same tier, as is also preferred for practice of the invention. (In this regard, however, it should be recognized that the assignment of any given tier to any given node is arbitrary.) For example, node 440 can communicate with node 450 over communication links 427, 423, 419 and 421; 427, 415, 418 and 425; or 427, 419, 417 and 425. Other redundant paths would exist if the network were extended to more tiers and/or more nodes per tier.

Therefore, routers monitoring traffic on the network can assign any of a number of convenient paths between any two nodes of the network. Conventional network protocols, in fact, allow a plurality of different paths that may be of differing latency to be employed for a given message with the bit packets being reassembled in proper order after receipt by the intended destination node. The invention provides the additional functionality of eliminating and substituting paths for isolation of questionable or compromised nodes at the portal or gateway to each node to maintain substantially full network functionality while preventing proliferation of faults or damage from attacks as well as the attacks themselves.

The locally hierarchical architecture described above greatly enhances security throughout the network since a response to an attack on one node will be controlled by another node which should respond correctly unless that node is simultaneously under attack, as well (prior faults throughout the network having been

previously encapsulated and isolated). In such a case, a manager object at yet another node at a locally higher hierarchical level would control the active response, and so on, while establishing a plurality of secure sessions and security domains (e.g. depicted by links 427, 415, 418, 425 of Figure 3 between node 440 and node 450 as client and server and which may be defined by the user or automatically as an incident of routing or re-routing communications) over which control can be exercised through user transparent communications from a manager object at a node which remains trusted. A plurality of levels of trust can also be readily implemented for respective nodes and communicated throughout the network system or any desired portion thereof.

In the event of a security breach, the CMIP managers possess the ability (in the manager objects) to instruct the SPM device to enable and disable network ports to isolate network nodes or segments/sectors and to notify other trusted entities in the CMIP manager and managed object hierarchy of changes in trust for potentially contaminated or compromised network devices while the remainder of the trusted devices of the network continue to provide services over redundant links and newly defined and substituted security domains while denying connection requests from untrusted sources, as can be seen from a comparison of Figures 2 and 3. Thus, protection from attacks by authorized users and against hijacked sessions, not previously available, can be provided as well as protection from attacks from other sources and of other types.

These communications and routing control can be carried out very rapidly (about twenty milliseconds per tier or less) and thus an active

TOP SECRET//EYES ONLY

response to a potential attack can be made in substantially real time and can be scaled to global size networks in log time. For example and as will be discussed in more detail below in connection with Figure 4, communications and control can be exercised over six tiers (or thirty-two nodes) in about 0.1 seconds and over eleven tiers (2048 nodes) in about 0.2 seconds. Therefore, global communications and active response to any number of attacks can be performed over even extremely large networks with interruptions, if any, sufficiently short as to be unnoticeable by a user. This is in sharp contrast to security arrangements in prior networks which typically could only log operations during an attack for later analysis long after the attack and damage resulting therefrom are completed.

By the same token, temporary disconnection of network segments or sectors to test for the origin and scope of an attack or to interrupt an attack may be made correspondingly short. Since the duration of any such disruption can be so short and the disruption thus minimized, very sensitive detection algorithms having relatively low initial confidence levels (but very rapid response) are tolerable for detection of potential attacks and to achieve a very high level of security. This capability provided by the present invention is particularly important in avoiding the effects of denial of service attacks which, by their nature, are difficult to distinguish from ordinary usage except by volume and possibly some similarity of transactions before such attacks are well under way and may have captured a significant portion of available resources.

Thus, an attack, to be successful, would require simultaneous attacks on virtually all

nodes of the system, all nodes of the hierarchically highest tier of the system or an attack on the hierarchically highest node (if such a singular node is permitted in the network
5 design; which is preferably avoided but should, in any case, be difficult to identify within the network since the relationships and dependencies in the network are identified only in the highly secure user-transparent communications between SPM cards which are preferably made difficult to intercept and analyze through high bit rate, low duty cycle transmissions and effective encryption). Such an attack would also need to be carried out simultaneously, if not synchronously,
10 at both the communicating, network connected processor level and at the SPM processor level of at least a plurality of processors since the manager and managed objects of the SPM processors are effectively self-repairing by virtue of the CORBA extensions for fault tolerance alluded to above.
15
20

It should be understood that the above discussion of compartmentalizing a portion of the network to isolate the location of a fault or an attack is merely exemplary of many types of active responses to such a fault or attack of which the invention makes the network capable through integration of the extended CORBA architecture which supports fault tolerance, strong encryption with user transparent communications which are difficult to intercept or simulate, implementation of attack detection at a lower level of certainty/higher level of sensitivity and speed for log time response and a fully flexible security policy capability.
25
30
35

Referring now to Figure 4, further exemplary capabilities of the invention will now be

discussed. It should be understood that Figure 4 is intended to depict an expansion of Figure 3 to a larger segment of a network system. That is, for reference, the segment of the network system depicted in Figure 3 is indicated by dashed line 300 in Figure 4 but could correspond to a similar group of nine contiguous nodes at any location in Figure 4 or the remainder of the network of Figure 4 beyond the nodes actually depicted. It is also to be understood that the functions depicted by other dashed lines in the expanded Figure 4 are concurrently available and may be executed simultaneously in accordance with the invention since the SPM devices/cards can operate autonomously and yet cooperate in many functions by virtue of the CORBA extensions engendering fault tolerance which are leveraged by the invention to provide enhanced security and an active response to attacks in log time.

It should also be understood that while the depiction of the network of Figure 4 is of planar topology insofar as the nodes which are depicted and a hierarchy of tiers is provided, only a locally hierarchical relationship between nodes is required and then only to the extent of ensuring an orderly relationship between manager objects and managed objects at different but connected nodes. Further, if it is desired to have a single node (which, if provided, is as fully secured as possible) for exercise of ultimate network security control and supervision at a higher hierarchical level than any other node, as alluded to above, the organization of the network system could be may triangular or pyramidal as depicted by chain line 301.

In this regard, it should be appreciated that if the tiered hierarchy is maintained globally

throughout the network, either in a planar or pyramidal organization, managed objects are only required for tiers 1 through N-1 and manager objects are only required for tiers 2 through N.

5 It is also desirable that the manager objects in any tier be able to communicate with each other for various purposes (and, preferably and advantageously, through a hierarchically higher tier), examples of which will be discussed below.

10 However, in a pyramidal arrangement where node 320 is of a higher hierarchical rank than any other node, such intra-tier communications will not be necessary (or possible) but other supervisory functions, the natures of which are unimportant to the successful practice of the invention and appropriate functions will, in any event, be evident to those skilled in the art, may be desirable in the manager objects of node 320.

15 As described above with reference to Figure 3, the isolation and encapsulation of node 409 is exemplary of perhaps the most elementary of active responses provided by the invention. It should be appreciated that the provision of the capability of any active response is a substantial advance over known security systems which typically merely log the fact of an attack or the portion of the operations carried out during the attack (while the node remains operational) for later analysis by trained security personnel in order to

20 determine the scope of damage and/or access which may have occurred. However, the invention provides and supports a wide variety of active responses in substantially real time (log time) to environmental changes and security related events,

25 illustrative examples of which will now be described. Again, all of these functions can be performed simultaneously and in log time.

09972776 - 101101
The ability to create layered security domains (by which management communications traffic is separated user data traffic and is maintained transparent to users) is fully
5 generalized in accordance with the principles of the invention at both the node or terminal processor (e.g. 119 of Figure 1) and the SPM processor. Since the managed and manager objects in the SPM processors are substantially and rapidly self-repairing, as discussed above, through the CORBA extensions for fault tolerance, any node can reach the SPM processor over a security domain which is not under simultaneous attack and which is beyond the security domains
10 involved in a particular network communication between a client and server.

For example, in links between client C and Server S and a potential attack A is detected at node 330, the scenarios discussed above in regard to Figure 3 would normally dictate that the security threat would be handled by the SPM device at node 331. Additionally, node 331 could communicate with other SPM devices in the same tier (e.g. at nodes 334 and 335) to revise the definition of the trusted and untrusted nodes, terminals and the like in the network environment and test downwardly through the tiers to determine the scope of the attack and the nature and timing of the response to be made. Thus, supervisory
20 evaluation, judgement and control is exercised by a node which is not included in the secure sessions involved in any particular communication or attack but which is exercised through communications through other secure domains used
25 by the user-transparent signals which are, themselves, highly secure.

30
35 If, however, node 331 was simultaneously

attacked (A'), the user transparent signals (depicted by dashed double arrows) would be communicated to a node 332 and/or 333 of the next higher tier, and so on, and diagnostics (e.g. as described in regard to nodes 334 and 335) and control manager objects run at other nodes of the tier at which a trusted node is found.

Thus, control and diagnostics can always be found unless simultaneous attacks are made on all nodes of at least three tiers of the network, while the organization of the tiers and connectivity of the nodes is hidden by user transparent and secure communications between the SPMs which also have the capability to detect "foreign" SPMs or connections since each link between SPMs is a secure domain. By the same token, any node or group of nodes can be rapidly isolated and the attack or fault compartmentalized very quickly in log time since communication, fault evaluation and control can be communicated through the user transparent signals between SPMs in about 20 milliseconds per tier or less. Known search techniques (e.g. binary trees) can propagate search and control to encapsulate any attack to affected nodes in very short log time even for extremely large and even global networks.

It should also be appreciated that the isolation provided in accordance with the invention allows the offending or questionable communications to be pushed back by interrupting communications not only with the connected nodes of the network depicted in Figure 4 but from other networks and/or connections to any particular node thereof. Thus the invention provides detection of questionable activities at every node, automatically collecting information related to any potential attack, isolation of the offending

TOP SECRET//EYES ONLY

object with arbitrary flexibility of response (e.g. flexibly determining the level of certainty of an attack for initiation of a response in accordance with the number of nodes to be

5 partitioned that is determined by the collected data concerning the potential attack), changing trust relationships between security domains, limiting the attack and even launching offensive information warfare capabilities (e.g. outbound
10 from the compromised node while limiting or eliminating inbound communications). Such protection is available and can be provided simultaneously over other groups of nodes of arbitrary extent and which can overlap, as
15 illustrated at 336 and 337.

Additionally, the ability to define security domains and secure sessions (and trust levels thereof) can be used not only to compartmentalize and isolate faults but can establish virtual
20 private networks (VPNs) somewhat similar to the third layer of protection provided by physically isolated systems described above except that the connectivity is user or administrator defined and may be altered at will to include resources at
25 desired nodes, as depicted at 340, while locking out all communications from other potential links. VPNs can be based, for example, on existing hardware and software products that implement to
30 the IPsec protocol suite and invoked by the user transparent communications and the above-described CORBA extensions.

The above-described security functions are fully available within the virtual private network including the ability to detect the connection of a "foreign" node communication in any security domain in the VPN, as described above, if included in the managed objects of included nodes, as would

TOP SECRET//SI

generally be the case. Of course, communications through some nodes not necessarily included in the VPN (e.g. nodes 341, 342) may be necessary but such communications do not lessen security of the
5 VPN since connection is made through locked routers. Redundant connections are provided and supervision is conducted in the manner described above at yet additional nodes in other layers; providing plural layers of protection around the
10 VPN. Thus a VPN provided in accordance with the principles of the invention is significantly more secure than a physically isolated network since protection is provided against session hijacking and attacks by authorized users.

15 It should be appreciated that the invention can develop defined VPNs in log time since the mechanism for defining the security domains is substantially the same as for compartmentalization and isolation but for the origin (e.g. with a user or administrator) of the VPN definitions. A useful application is to provide security for critical resources through the security policy manager during normal network operation and to switch to VPNs if an attack is detected in the
20 network or critical segments thereof. This switching to VPNs would have the effect of terminating service to users having authorization for less than all of the resources of nodes in the VPN and effectively increase protection against
25 attacks by authorized users.

30 In view of the foregoing, it is seen that the invention provides a capability of dynamic active response in log time to detected security events and fault conditions while allowing tailoring of responses in a manner commensurate with risk and system disturbance required to fully and
35 effectively address any attack. The response may

100-9777-6960

be offensive, defensive or both and the actions taken may be flexibly defined and timed since the function of the invention to detect attacks and initiate active responses is entirely independent
5 of the conditions detected and the nature of the responses. This active response capability is integrated with and leveraged by all components of the architecture of the invention as implemented within an arbitrary network and with arbitrarily fine granularity.

10 While the invention has been described in terms of a single preferred embodiment, those skilled in the art will recognize that the invention can be practiced with modification
15 within the spirit and scope of the appended claims.